CLAIMS:

1 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" using authentication codes and portable verifier elements which can process and store information and which offer a high level of protection against unauthorized readers and writers. The method is characterised in that the aforementioned authentication code is generated specifically for a particular portable verifier and is indicated directly or indirectly by the person requesting the document. In this way, no data record of any type is required in the portable verifier element up to the point at which the document is validated. It is essential, however, that the portable verifier be actively involved in the validation, said portable verifier containing a stored list of validated documents such that it is possible to determine, at least, whether or not this is the first validation.

2 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the first claim and characterized in that it is comprised on two stages:

- The portable verifier devices are individualized by the senders using one or more keys of the portable verifier device.
- The document is generated from a document portal and the data considered relevant is coded using the key that corresponds to the group of readers/verifiers/recorders involved in the validation of the document, so that the first cryptographic operation can be carried out. Linked to the first one, there is another second cryptographic operation which includes the key corresponding to the portable verifier device associated with the document, and, as a result of these cryptographic operations, an authentication code is created for the document and is incorporated therein; and
- The document is checked by reader its authentication code, and the appropriate third cryptographic operations are carried out to verify those already employed to generate the document. It is essential, however, that the portable verifier device associated for the validation of the document be actively involved, and said portable verifier should contain a list of validated documents such that it is possible to determine, at least, whether or not this is the first validation.

3 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that:

- The individualization phase of the portable verifier devices is carried out by storing one or more portable verifier device keys, which must be an symmetric or secret key encryption algorithm;
- The first and second cryptographic operations are made up of two encryptions using a symmetric cryptographic algorithm, one using the key of the group of readers/verifiers/recorders involved in the validation of the document and the other using the key that corresponds to the portable verifier device associated with the document, and in that;
- The third cryptographic operations consist of decrypting, by the portable verifier device using its corresponding key, of the document's authentication code and the subsequent decryption, carried out by the aforementioned

reader/verifier/recorder and its corresponding code. Both decryptions will be effected through symmetric cryptographic algorithms.

4 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that:

- The portable verifier devices should be individualized by storing one or more portable verifier device keys, which must be the secret keys of an asymmetric or public key cryptographic algorithm;
- The abovedescribed first and second cryptographic operations are based on public key cryptography which is composed of a digital signature with a secret key, and the readers/verifiers/recorders involved in the validation of the document will know its corresponding public key, and an encryption using the corresponding public key of the portable verifier device associated with the document; and in that
- The third cryptographic operations will be based on public key cryptography composed of a decryption using the secret key corresponding to the portable verifier device associated with the document and the verification of the signature, using the corresponding public key stored in the readers/verifiers/recorders.

5 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that:

- The portable verifier devices should be individualized by storing one or more portable verifier device keys, which must be the secret keys of an asymmetric or public key cryptographic algorithm;
- The abovedescribed first and second cryptographic operations are based on public key cryptography which is composed of an encryption using the public key of the readers/verifiers/recorders involved in the validation of the document, and an encryption using the corresponding public key of the portable verifier device associated with the document; and
- The third cryptographic operations will be based on public key cryptography composed of a decryption using the secret key corresponding to the portable verifier device associated with the document and a decryption using the secret key of the readers/verifiers/recorders.

6 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that

- The portable verifier devices should be individualized by storing one or more portable verifier device keys, which must be the public keys of an asymmetric or public key cryptographic algorithm;
- The abovedescribed first and second cryptographic operations are based on public key cryptography which is composed of digital signature using the secret key that corresponds to the public key stored in the readers/verifiers/recorders involved in the validation of the document, and another digital signature using the secret key corresponding to the appropriate individualization key stored in the portable verifier device associated with the document; and

- The third cryptographic operations will be based on public key cryptography composed of the verification of the signature by the portable verifier device associated with the document using the appropriate individualization key and a second verification of the signature using the public key of the readers/verifiers/recorders.

7 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that

- The portable verifier devices are individualized by storing one or more portable verifier device keys, which must be the public keys of an asymmetric or public key cryptographic algorithm;
- The first and second cryptographic operations are based on public key cryptography which is composed of an encryption using the public key corresponding to the secret key stored in the readers/verifiers/recorders involved in the validation of the document and a digital signature using the secret key corresponding to the appropriate individualization key stored in the portable verifier device associated with the document; and in that
- The third cryptographic operations will be based on public key cryptography composed of the verification of the signature by the portable verifier device associated with the document using the appropriate individualization key and a decryption using the secret key corresponding to the readers/verifiers/recorders.

8 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any other the above claims, is characterized in that it consists of the checking, before the document is validated, that it is not already included in the list of validated documents.

9 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the eighth claim and characterized in that the reader/verifier/recorder is informed if the document to be validated in already included in the list of validated documents, so that it can proceed as appropriate.

10 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the eighth claim and characterized in that the document to be validated will then be included in the list of validated documents, provided it was not already there, and the corresponding cryptographic operation will be carried out when reversing and/or checking the cryptographic operation corresponding to the portable verifier device, and the result is sent to the reader/verifier/recorder so that it can proceed as appropriate

11 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that the cryptographic authentication established between the portable verifier device and the reader/verifier/recorder is mutual and firm

12 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the eleventh claim and characterized in that a cooperative and random session key is established between the portable verifier device and the reader/verifier/recorder and is used to encrypt the pertinent messages between the two.

13 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that the portable verifier devices are individualized by the senders using one or more keys obtained from the encryption of the serial number with one or more master keys chosen by the portable verifier device operators, so that the master key of each operator and the portable verifier device corresponds to the identifier, which should be legible by the user.

14 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that the abovementioned reader/verifier/recorder has been adapted to send information, accepting or rejecting the document and stating the reason why.

15 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that the reader/verifier/recorder keys are common to the group of readers.

16 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the second claim and characterized in that the keys stored in the readers/verifiers/recorders are obtained by encrypting the identifiers, or parts of these, using the master keys chosen by the operators.

17 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the first claim and characterized in that in the event the document has an expiry date, this will be included in the authentication code, so that they can be eliminated from the list of validated documents stored in the portable verifier once this date has passed.

18 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with the seventeenth claim and characterized in that said portable verifier devices receive the date expired documents are to be deleted from the list of validated documents through a digital certificate sent by a competent body.

19 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that the document and/or authentication code can be selected and obtained through Internet.

20 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that the document's authentication code can be sent to the user's mobile telephone.

21 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that the document's authentication code can be sent to the user's electronic agenda, or any other similar device belonging to the user

22 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that the authentication code can be printed through a barcode.

23 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that in that the authentication code can be printed through one or more barcodes.

24 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that the authentication code can be printed through an alphanumerical code.

25 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with any of the previous claims and characterized in that the authentication code can be printed through a dot code.

26 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with twenty second and twenty fifth claims and characterized in that the authentication code can also be printed through an alphanumerical code so that it can by keyed in manually in the event the automatic reading code deteriorates.

27 – "METHOD OF SENDING AND VALIDATING DOCUMENTS" in accordance with twenty-third claim and characterized in that the barcodes include the correct reading order.